RSAC 2025 Conference

Many Voices.
One Community.

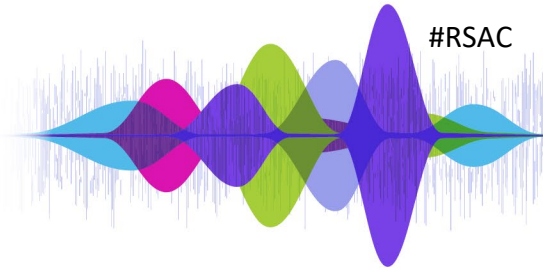
SESSION ID: HT-W09

Initial Access Brokers: A Deep Dive

Amit Weigman

Head of Solution Engineering
Cyberint (now a Check Point company)

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

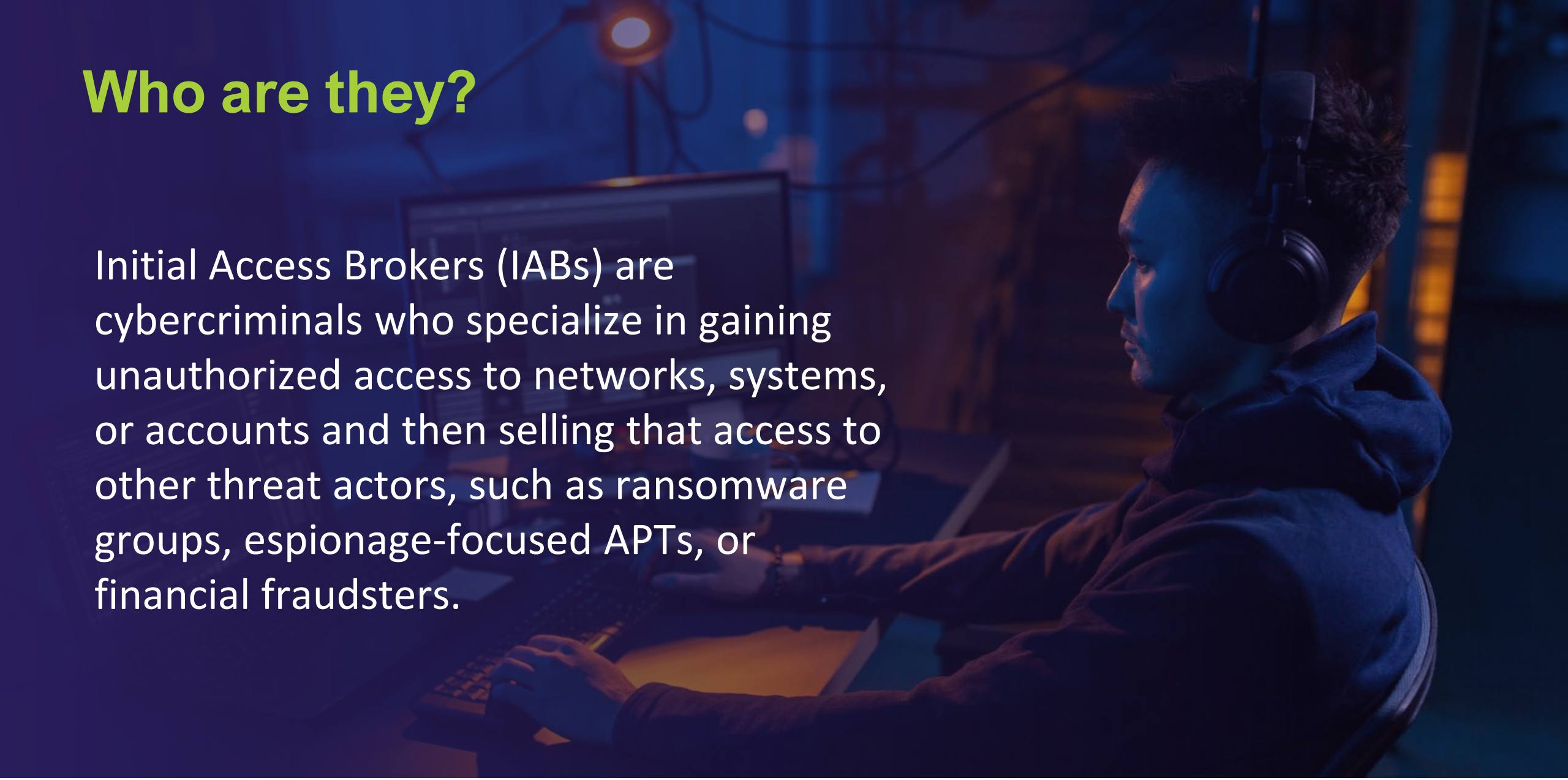
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda

- Introduction
- Who Are The IABs?
- Sources of Operations
- Statistics – Worldwide & USA Focus
- Threat Actors Profiling & Attacks
- Impact
- Conclusions & Predictions

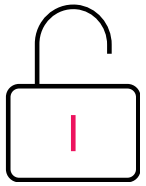
Who are they?



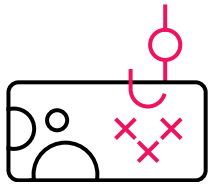
Initial Access Brokers (IABs) are cybercriminals who specialize in gaining unauthorized access to networks, systems, or accounts and then selling that access to other threat actors, such as ransomware groups, espionage-focused APTs, or financial fraudsters.

How they Operate

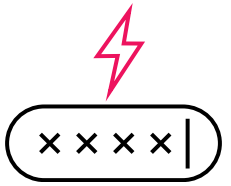
Gaining Access



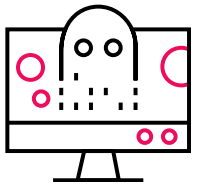
Exploiting vulnerabilities (Mostly RCE)



Phishing attacks to steal credentials



Credential stuffing or brute force attacks



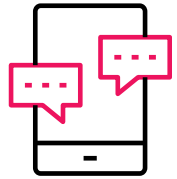
Malware infections (Info Stealers)

How they Operate

Selling the Access

Underground forums or darkweb marketplaces

Direct deals with ransomware operators / APTs



Telegram channels or invitations in darkweb closed groups

How they Operate

Selling the Access

Markets or Campaigns

Spam/ Other Markets

Opportunistic Attacks

$ 50 to 150

Initial Access Brokers

Grooming and Maturation

$ 500 to 10,000

Ransomware Affiliates

Deployment

$ Revenue Sharing

Ransomware Operators

Manage Negotiations

$ 10,000 to >1mln

RSAC™ 2025 Conference

Where?

Many Voices.
One Community.

Where they Operate

Darkweb Forums & Marketplaces - Advertising

- XSS.IS
- Forum.Exploit.in
- Breachforums.vc
- Ramp.io

Private Channels – Communication

- TOX
- Telegram
- Jabber
- Forums Private Chats (DMs)

XSS.IS

- **Language**: Predominantly Russian.
- **Date Started**: Initially launched as DaMaGeLaB in 2013; rebranded to XSS.is in September 2018 following the arrest of an administrator.
- **Main Topics**: Discussions focus on malware, exploits, vulnerabilities, carding, and a live marketplace for accesses, combo lists, and more.
- **Accessibility**: The forum can be accessed via both the clear web and the dark web, with registration requiring administrative approval.
- **Political Stance**: The forum often supports Russia's political positions, notably evident during the onset of the Russia-Ukraine conflict.

Forum.Exploit.in

- **Language:** Primarily Russian.
- **Date Started:** 2005.
- **Main Topics:** The forum is a marketplace for trading illicit goods and services, including stolen personal data, credit card information, botnets, phishing kits, hacking tools, exploits, database leaks, cryptocurrency discussions, and anonymity techniques.
- **Membership:** Known for its exclusivity, requiring invitations and fees for registration. Non-Russian speakers and inexperienced users are generally discouraged from joining.

Ramp.io

- **Language:** The forum primarily operates in Russian.
- **Date Started:** The original RAMP forum was launched in 2020. It was relaunched on August 13, 2021, with registration available under specific criteria.
- **Registration:** Users need a 2-month-old account with 10+ posts on XSS or Exploit forums and a good reputation. Alternatively, anonymous registration costs $500, higher than most forums.
- **Main Topics:** The forum centers on Ransomware-as-a-Service (RaaS), malware trading, data leaks, and stolen info. The admin also seeks professionals for security audits.

Breachforums.st

BF

- **Language:** English
- **Date Started:** March 2022- Launched as a successor to **RaidForums.**
- **Registration Requirements:** As of May 2024, visitors are required to create an account to access the forum's content. This change has led to speculation about the forum's intentions and potential security risks for users.
- **Main Topics:** Data breaches, hacking tools, and cybercrime services
- **Arrests:** Founder Conor Brian Fitzpatrick (alias "pompompurin") was arrested in March 2023. Subsequent administrator "Baphomet" was reportedly arrested in May 2024.

RSAC™ 2025 Conference

Access for Sale

a live example

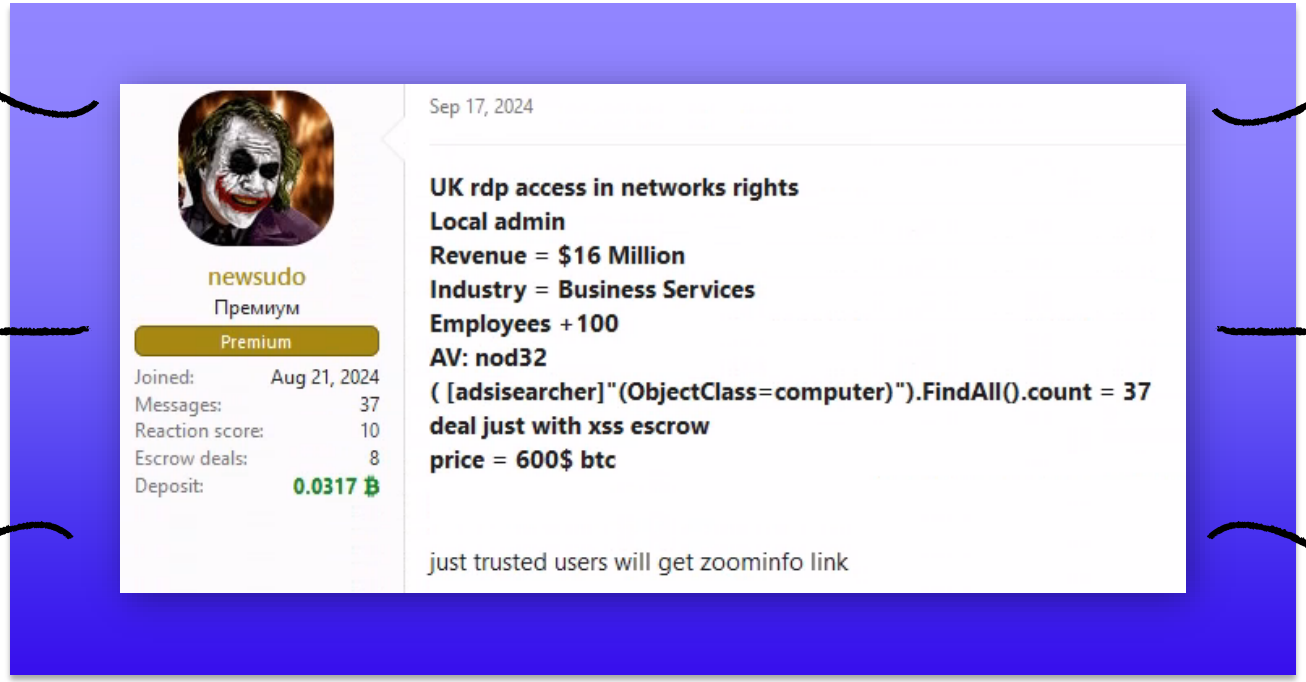
Many Voices.
One Community.

Access for Sale Breakdown

Access Type:
RDP, VPN, Web Panel, SSH, Email – Citrix, Fortinet.

Victim Industry:
Business Services, Finance, Education, Manufacturing, etc.

Victim Location:
Country or region of the affected organization.



Revenue:
The annual revenue of the victim company.

Number of Employees:
Size of the compromised organization.

Privileges:
Local User, Domain Admin, User in Domain, etc.

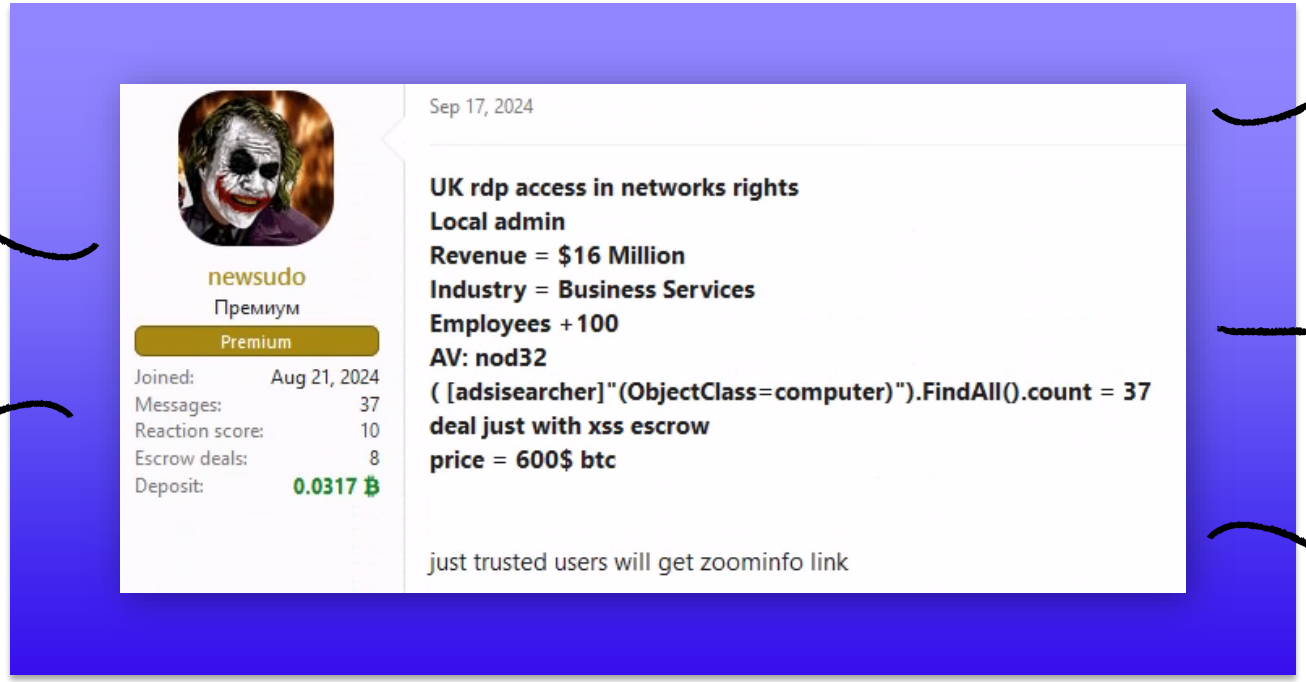
Access for Sale Breakdown

Endpoints/ Hosts:

Number of machines or network assets accessible.

Security Software:

EDR, AV, or firewall detected.



Exfiltration Potential:

Data theft possibility, databases, backups.

Additional Services:

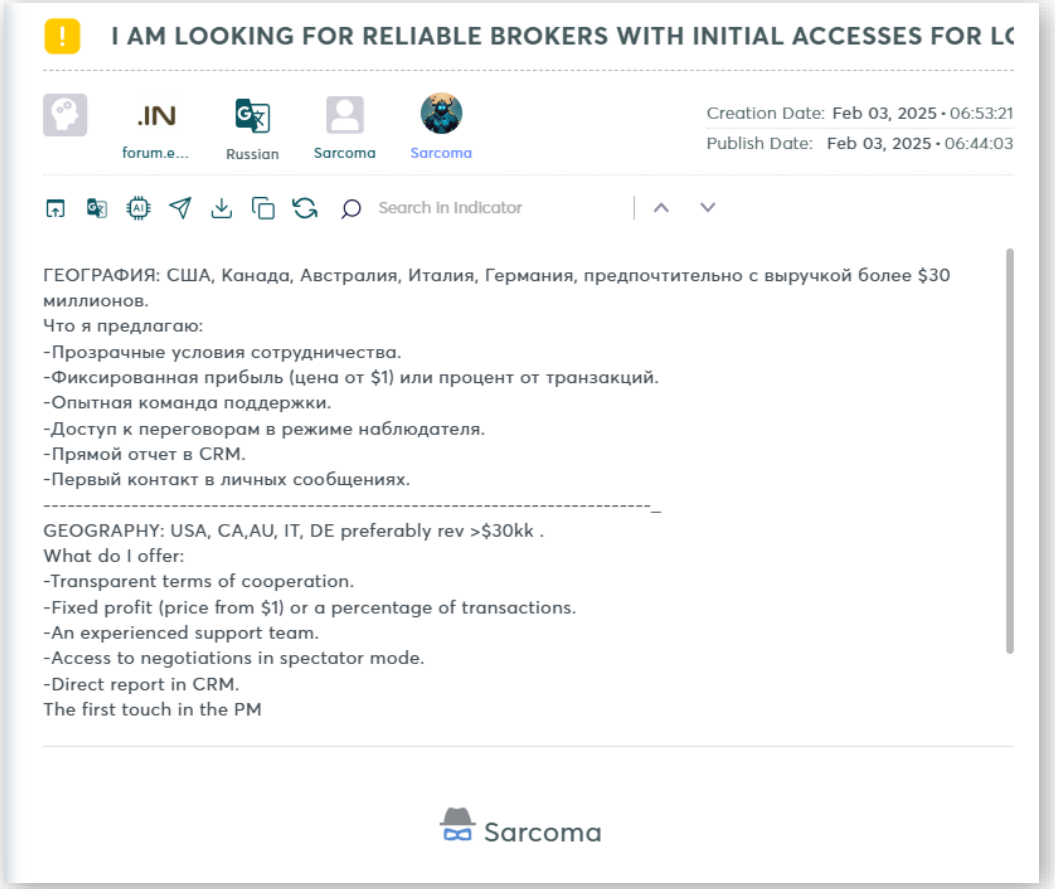
Lateral movement, privilege escalation, etc.

Price:

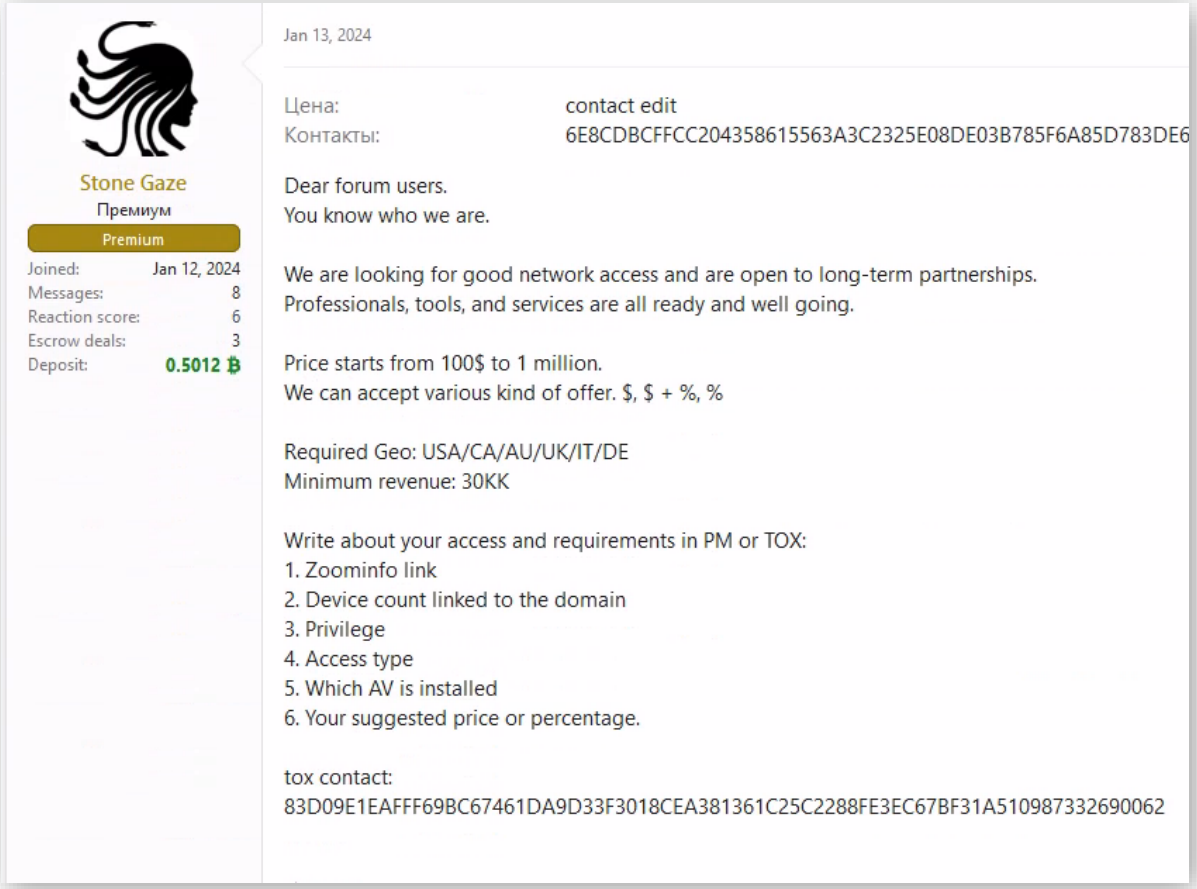
Cost of access

Ransomware Groups Search for Access

Sarcoma Group

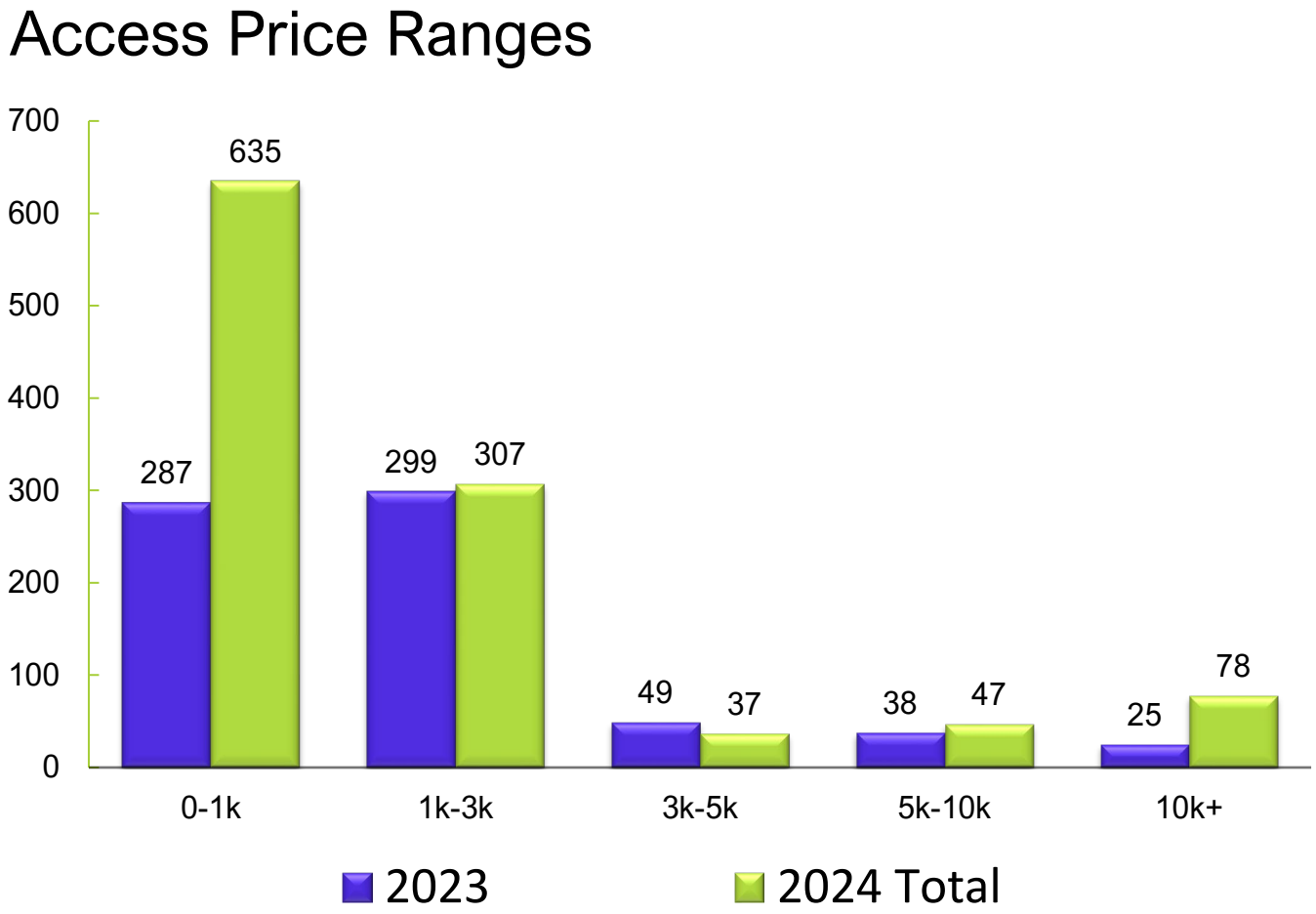

I AM LOOKING FOR RELIABLE BROKERS WITH INITIAL ACCESSES FOR LC
.IN
forum.e...
Russian
Sarcoma
Sarcoma
Creation Date: Feb 03, 2025 • 06:53:21
Publish Date: Feb 03, 2025 • 06:44:03
Search in Indicator
ГЕОГРАФИЯ: США, Канада, Австралия, Италия, Германия, предпочтительно с выручкой более $30 миллионов.
Что я предлагаю:
-Прозрачные условия сотрудничества.
-Фиксированная прибыль (цена от $1) или процент от транзакций.
-Опытная команда поддержки.
-Доступ к переговорам в режиме наблюдателя.
-Прямой отчет в CRM.
-Первый контакт в личных сообщениях.
GEOGRAPHY: USA, CA,AU, IT, DE preferably rev >$30kk .
What do I offer:
-Transparent terms of cooperation.
-Fixed profit (price from $1) or a percentage of transactions.
-An experienced support team.
-Access to negotiations in spectator mode.
-Direct report in CRM.
The first touch in the PM
Sarcoma

Medusa Group


Stone Gaze
Премиум
Premium
Joined: Jan 12, 2024
Messages: 8
Reaction score: 6
Escrow deals: 3
Deposit: 0.5012 ₿
Jan 13, 2024
Цена: contact edit
Контакты: 6E8CDBCFFCC204358615563A3C2325E08DE03B785F6A85D783DE6
Dear forum users.
You know who we are.
We are looking for good network access and are open to long-term partnerships.
Professionals, tools, and services are all ready and well going.
Price starts from 100$ to 1 million.
We can accept various kind of offer. $, $ + %, %
Required Geo: USA/CA/AU/UK/IT/DE
Minimum revenue: 30KK
Write about your access and requirements in PM or TOX:
1. Zoominfo link
2. Device count linked to the domain
3. Privilege
4. Access type
5. Which AV is installed
6. Your suggested price or percentage.
tox contact:
83D09E1EAFFF69BC67461DA9D33F3018CEA381361C25C2288FE3EC67BF31A510987332690062

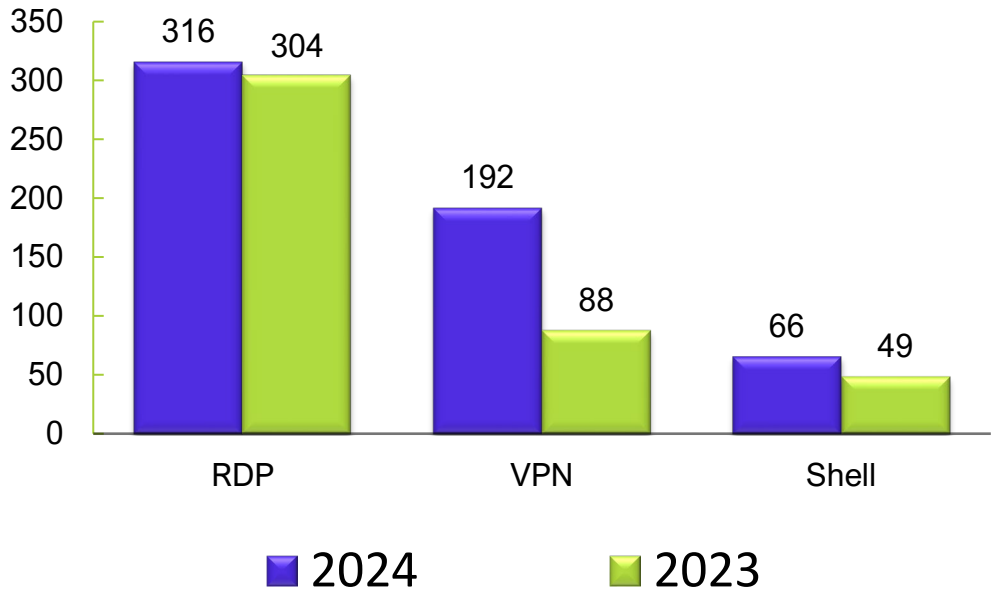
Stats – 2024 vs. 2023

- **Where is the highest relative increase?**

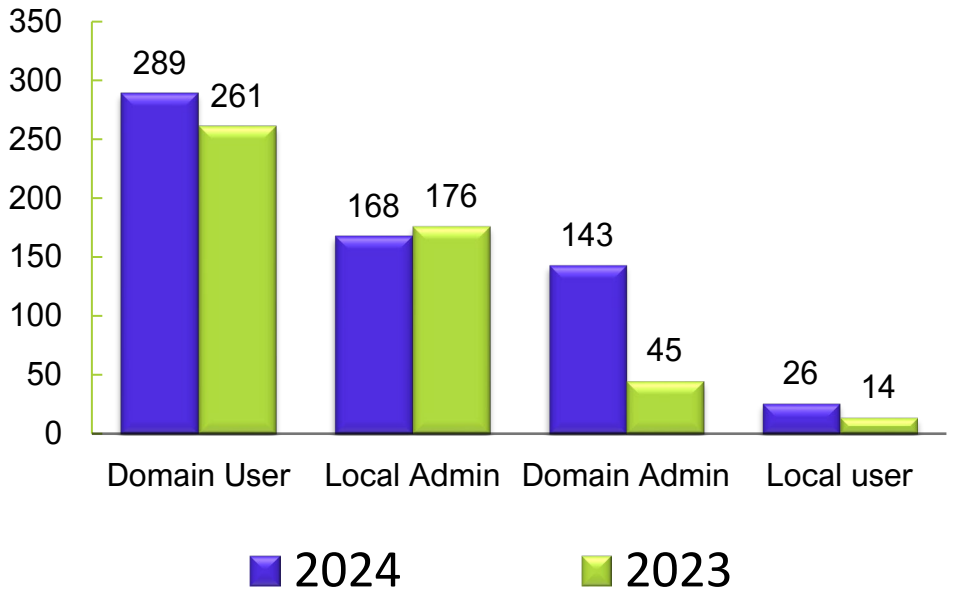


Stats – 2024 vs. 2023

Top 3 Access Types Offered for Sale



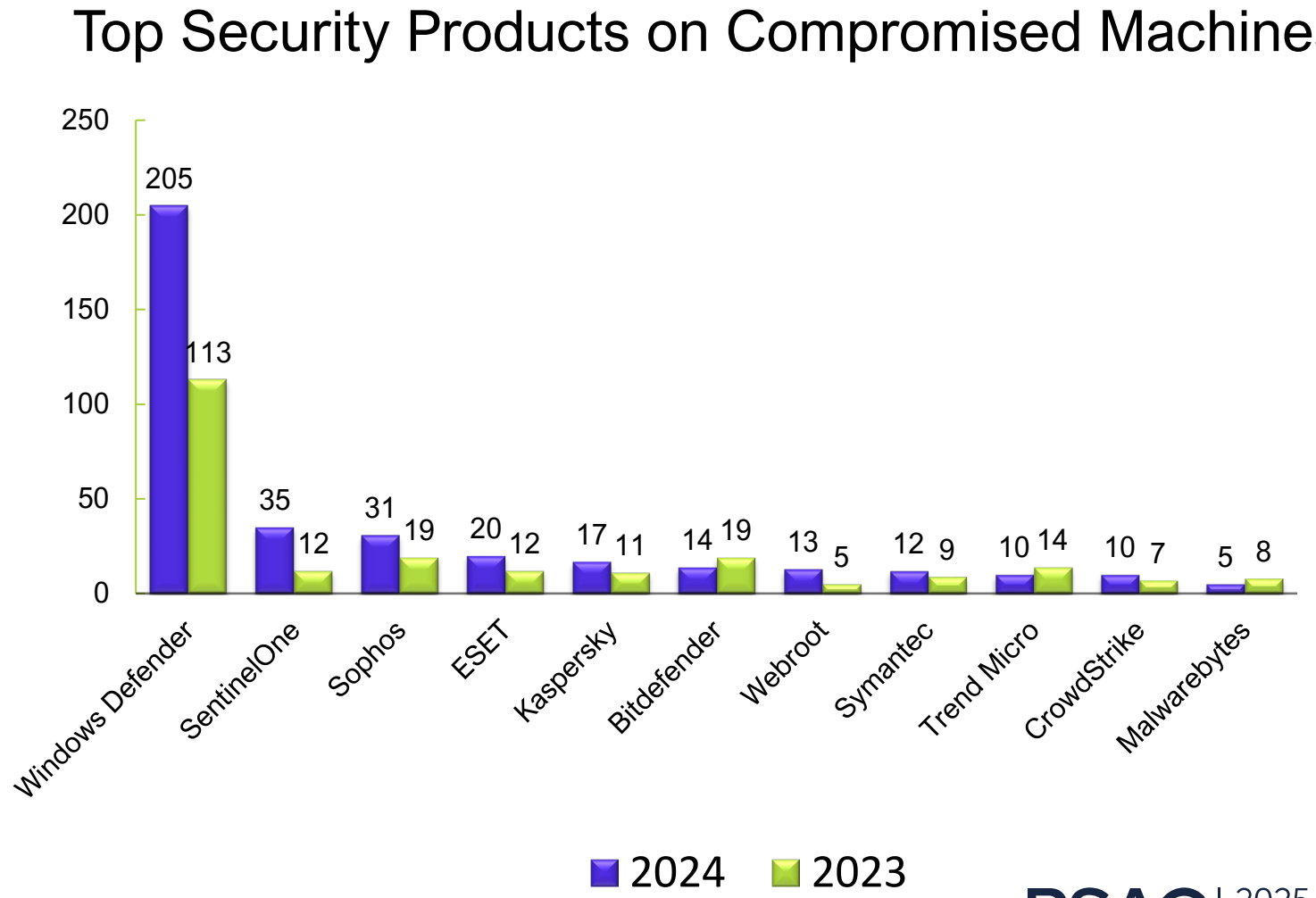
Top 3 Privileges Offered for Sale



- Connection using RDP/VPN, with Domain user/Local Admin are the most common accesses offered for sale
- **Top Platforms** – Citrix, FortiClient, AnyDesk, AnyConnect, Global Protect

Stats – 2024 vs. 2023

- In 2023 60% of the published accesses didn't contain the security product field
- In 2024 65% of the published accesses didn't contain the security product field
- Windows Defender is the most popular security product on compromised machines



Sources Comparison - 2024

Underground Platforms Comparison by Number of Accesses Offered for Sale

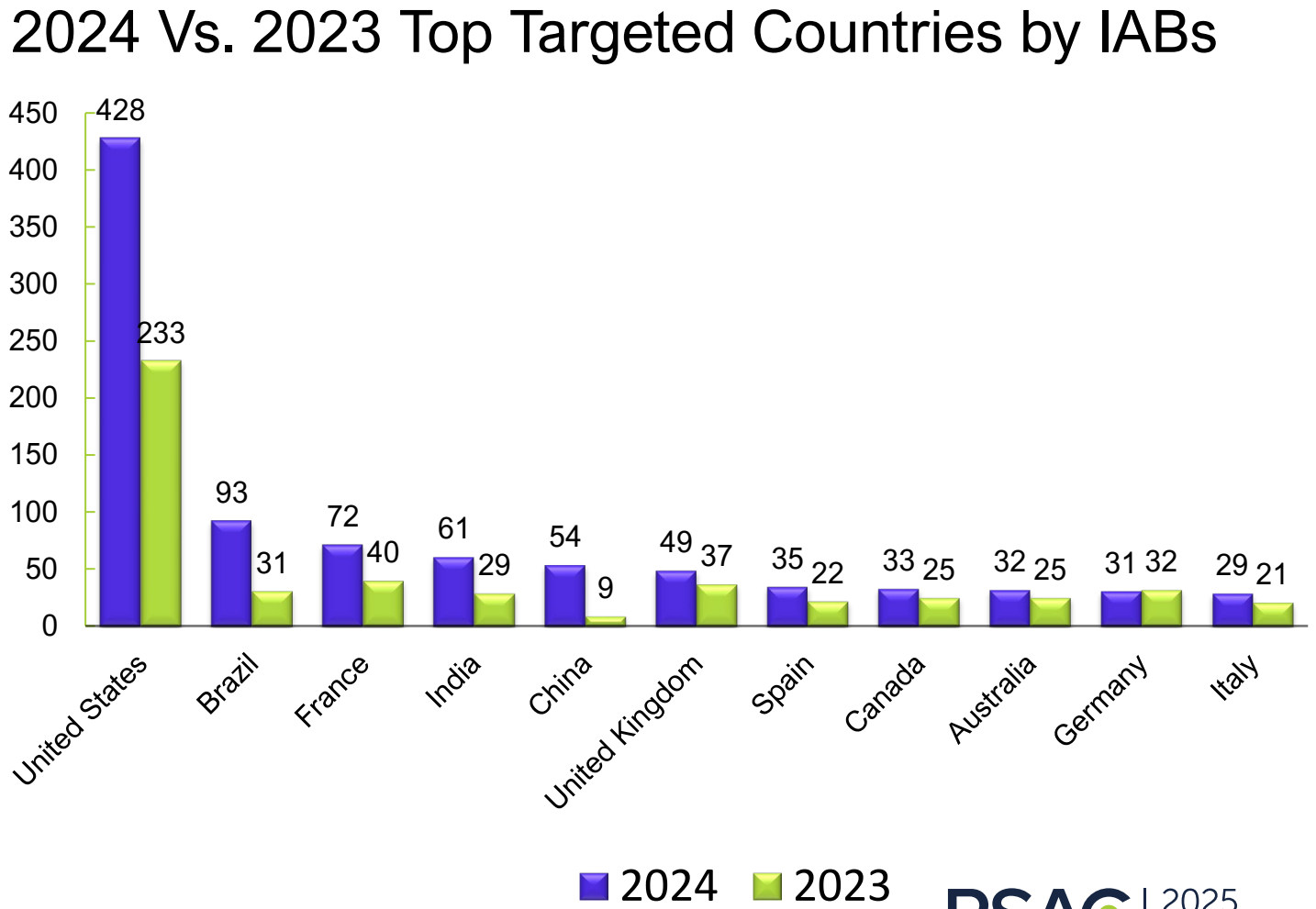
XSS.is	BreachForums	Ramp.io	Forum.Exploit.in
39%	28%	19%	14%

RSAC 2025 Conference

Target Analysis

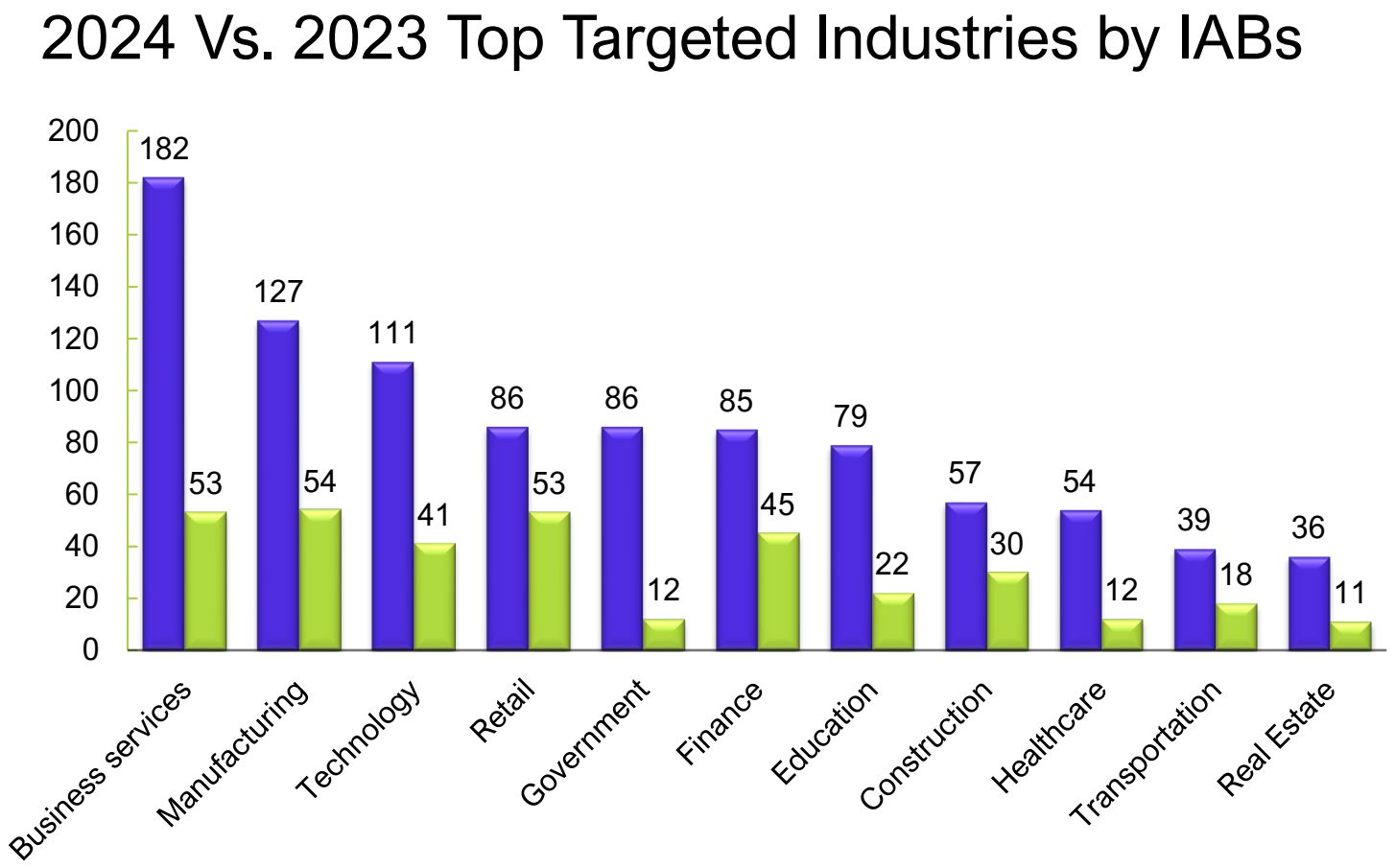
Stats – 2024 vs. 2023

- **Number of accesses for sale increased by 90% - but why?**



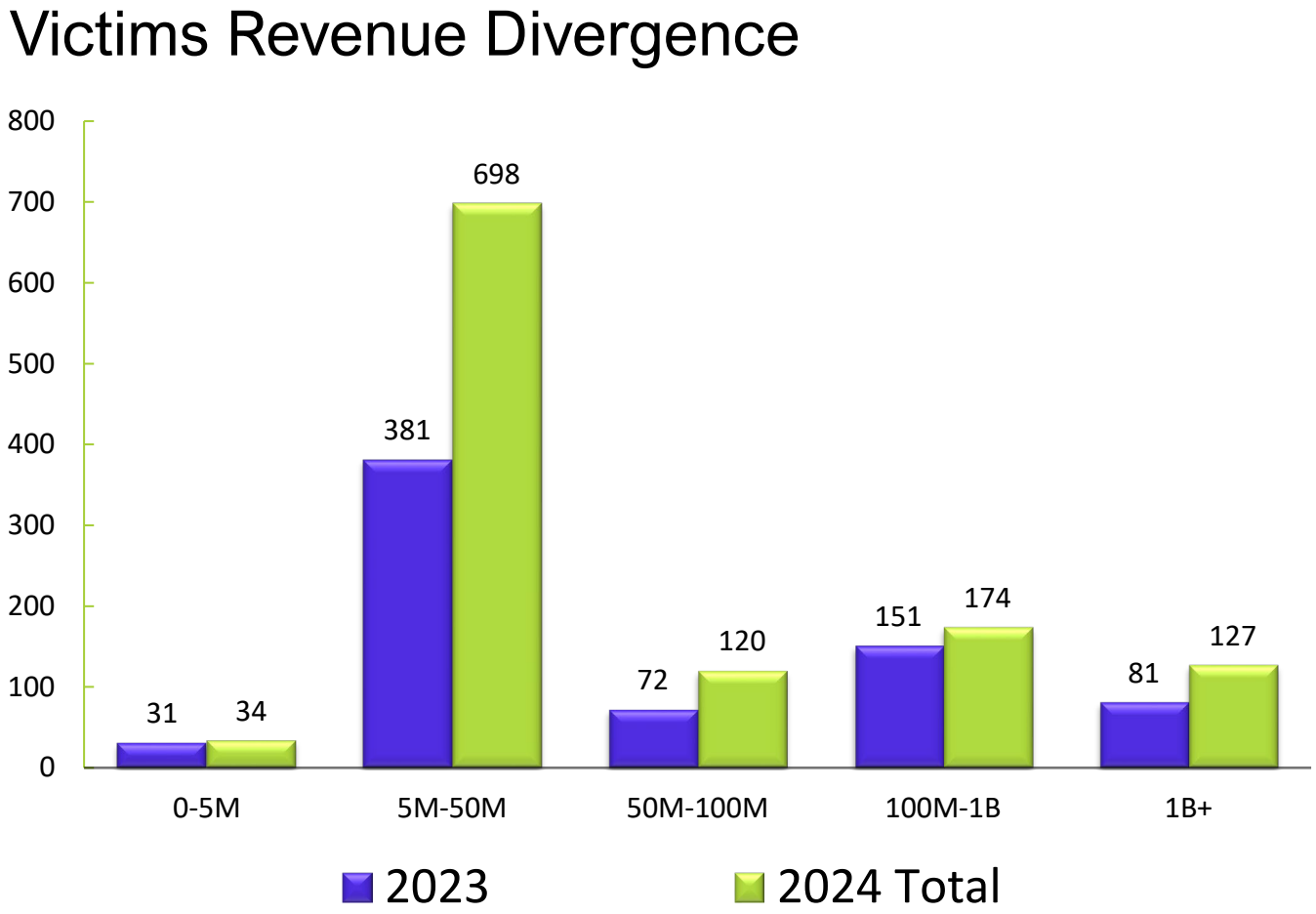
Stats – 2024 vs. 2023

- **What is the highest relative increase – but why?**



Stats – 2024 vs. 2023

- Average revenue 2023 – $1.38B
- Average revenue 2024 - $1.28B
- Median revenue 2023/2024 – 28M/19M
- 5M-50M Group – Increased by 83%
- 50M-100M Group – Increased by 66%
- 1B+ Group – Increased by 56%

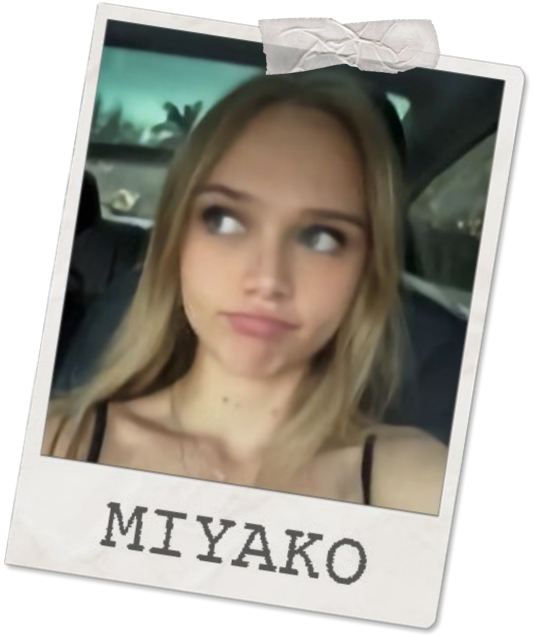


RSAC 2025 Conference

Threat Actor Profiling

Miyako

- **Name:** "Miyako" is derived from a Japanese term meaning "capital" or "city," reflecting its focus on critical infrastructure in urban and capital regions.
- **Origin:** There are signs of connections to East Asian cybercriminal forums and state-affiliated organizations.
- **Platforms:** Breachforums, X (Twitter), Asian Underground Forums
- **Motivation:** (?)
- **Significant Incidents:** FBI Subdivision, State University, USA Paper Manufacturer, $7B French Energy Distribution Company, Indonesian Government Financial Services



Miyako

[SOLD] FBI Subdivision
by miyak0 - Friday December 13, 2024 at 01:42 PM

Initial Access Broker

12-13-2024, 01:42 PM (This post was last modified: 12-14-2024, 08:26 AM by miyak0.)

Details:
Access to server hosting firewall in FBI Subdivision.

Privilege:
Root access to server

Revenue:
Unknown

Price:
$2000

Price is NOT negotiable. SERIOUS BUYERS ONLY

[SOLD] United States Air Force Base
by miyak0 - Wednesday December 11, 2024 at 07:32 PM

Initial Access Broker

12-11-2024, 07:32 PM (This post was last modified: 12-14-2024, 08:27 AM by miyak0.)

Details:
Access to server hosting firewall in United States Air Force Base.

Privilege:
Root access to server

Revenue:
Unknown

Price:
$800

Price is NOT negotiable. SERIOUS BUYERS ONLY

[SOLD] $17bil Revenue Major USA Manufacturing
by miyak0 - Friday December 6, 2024 at 10:42 AM

Initial Access Broker

12-06-2024, 10:42 AM (This post was last modified: 01-03-2025, 05:33 AM by miyak0.)

Details:
Access to server hosting firewall in Major USA Manufacturing.

Privilege:
Root access to server

Revenue:
$17bil

Price:
$700

$18bil Revenue Africa Government Petroleum
by miyak0 - Sunday December 1, 2024 at 06:14 AM

Initial Access Broker

12-01-2024, 06:14 AM (This post was last modified: 12-08-2024, 11:28 PM by miyak0.)

Details:
Access to server hosting firewall in Africa Government Petroleum.

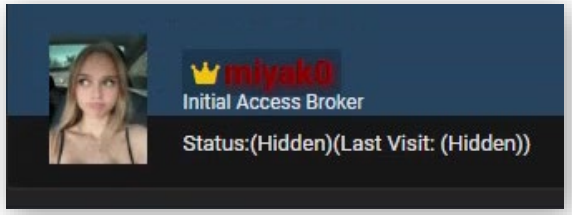
Privilege:
Root access to server

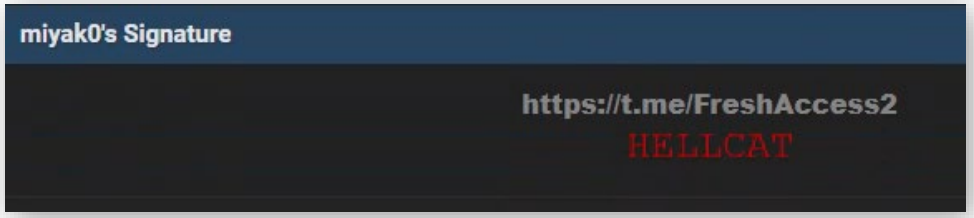
Revenue:
$18billion

Price:
$300

Miyako

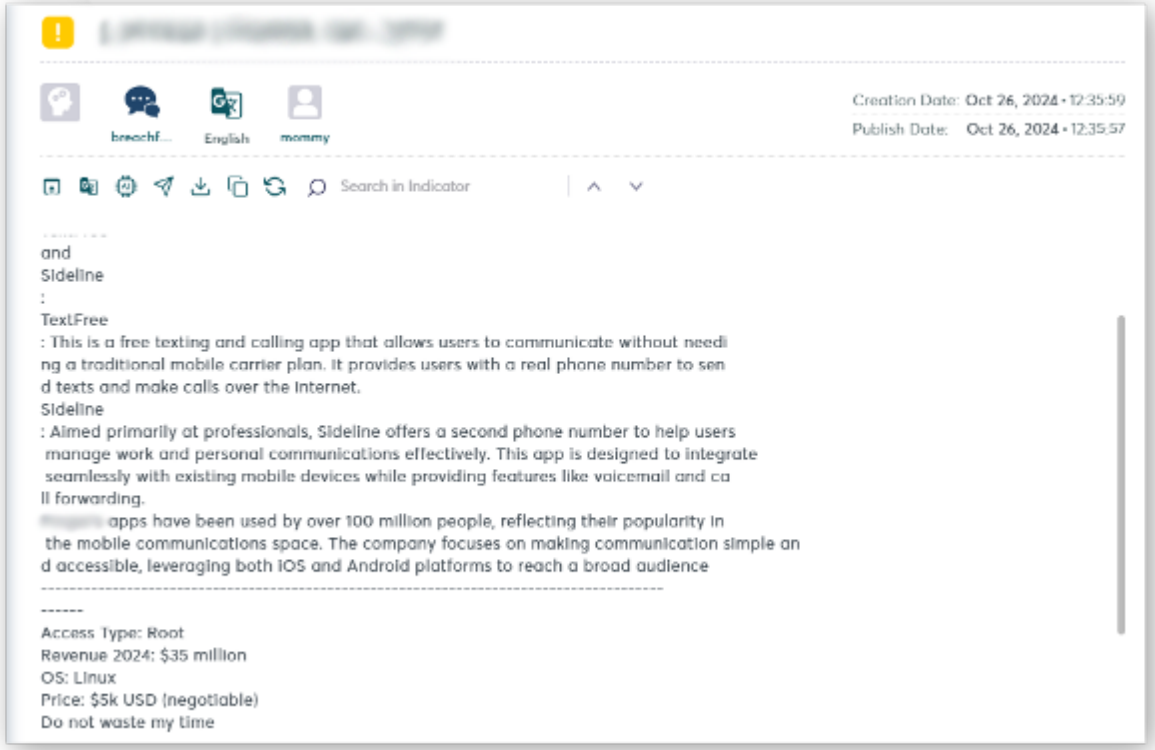
- **Targeted Industries:** Manufacturing, Telecommunications, Retail, Education, Government, Energy, Healthcare, Finance, Critical Infrastructure
- **Targeted Countries:** USA, China, France, Hong Kong, Iran, Germany, Ukraine, Hungary, Italy, Indonesia, Taiwan, South Korea, South Africa, Canada, Iraq, Brazil, Argentina, Mozambique
- **TTPs:** exploiting zero-days in firewalls and enterprise applications (GitLab (CVE-2024-45409)), Phishing , Exploitation of Public-Facing Applications, Manipulates legitimate user accounts to maintain access, Exploits misconfigurations in identity management systems like SAML
- **Average Price:** $562.50



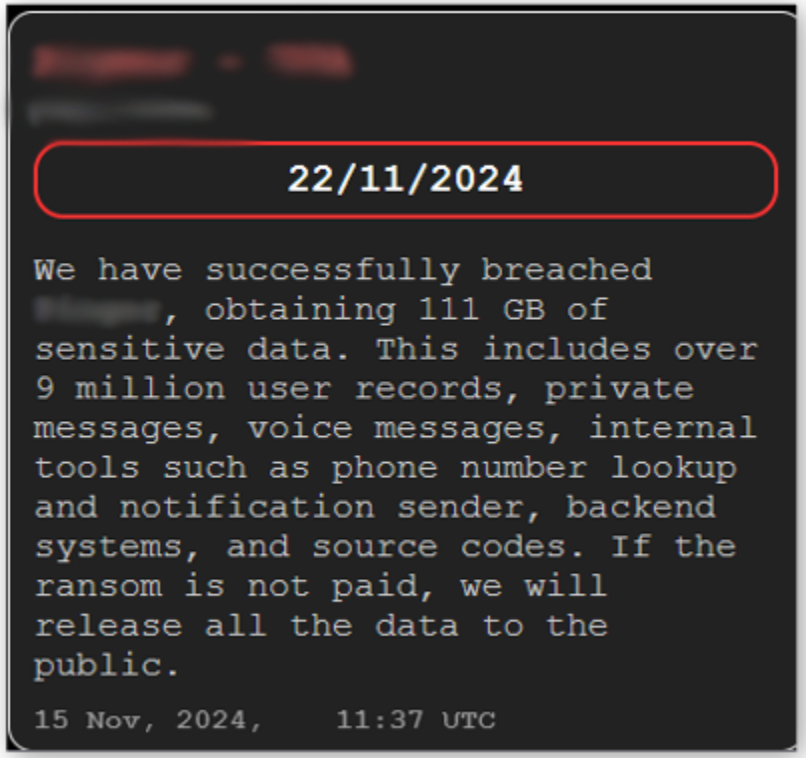


Pinger Ransomware Attack

Weeks before the attack, “mommy” or as we know him - “miyako”, leveraged CVE-2022-1388, a critical authentication bypass vulnerability in F5 BIG-IP devices.

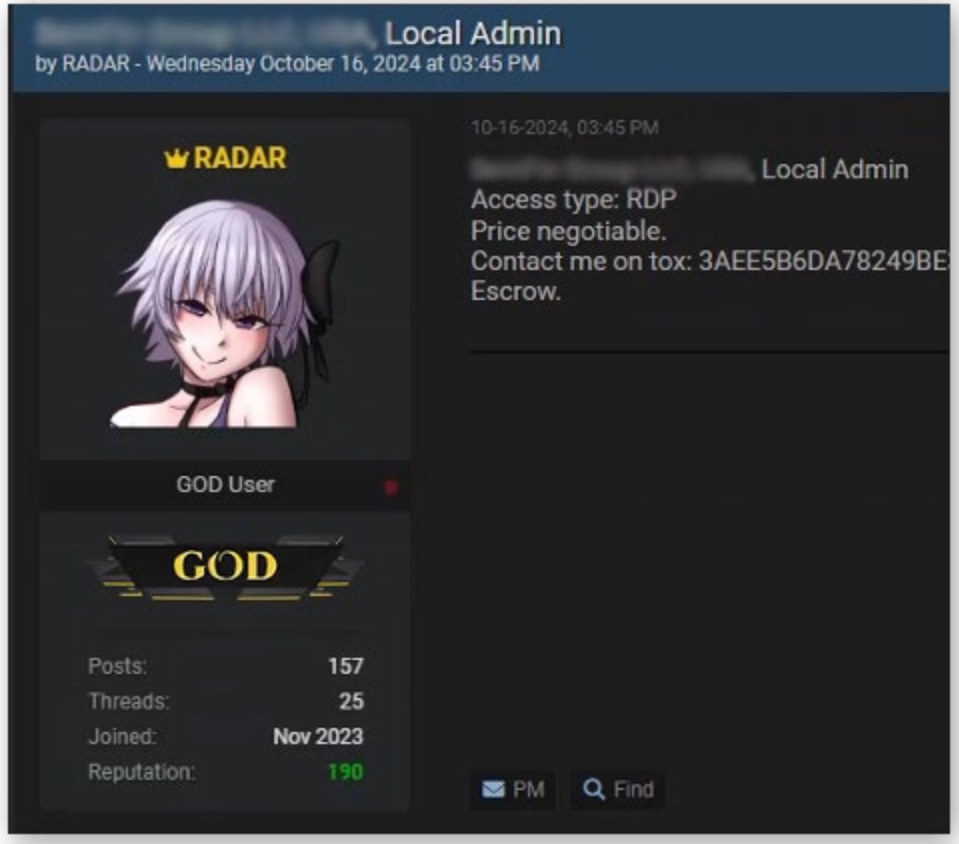

Creation Date: Oct 26, 2024 • 12:35:59
Publish Date: Oct 26, 2024 • 12:35:57
English
mommy
Search in Indicator
and
Sideline
:
TextFree
: This is a free texting and calling app that allows users to communicate without needi
ng a traditional mobile carrier plan. It provides users with a real phone number to sen
d texts and make calls over the Internet.
Sideline
: Aimed primarily at professionals, Sideline offers a second phone number to help users
manage work and personal communications effectively. This app is designed to integrate
seamlessly with existing mobile devices while providing features like voicemail and ca
ll forwarding.
apps have been used by over 100 million people, reflecting their popularity in
the mobile communications space. The company focuses on making communication simple an
d accessible, leveraging both iOS and Android platforms to reach a broad audience
---
Access Type: Root
Revenue 2024: $35 million
OS: Linux
Price: $5k USD (negotiable)
Do not waste my time

Hellcat Attack - ransom demand of **$150,000** in Monero or Bitcoin


22/11/2024
We have successfully breached
, obtaining 111 GB of
sensitive data. This includes over
9 million user records, private
messages, voice messages, internal
tools such as phone number lookup
and notification sender, backend
systems, and source codes. If the
ransom is not paid, we will
release all the data to the
public.
15 Nov, 2024, 11:37 UTC

Swiss Corp Ransomware Attack

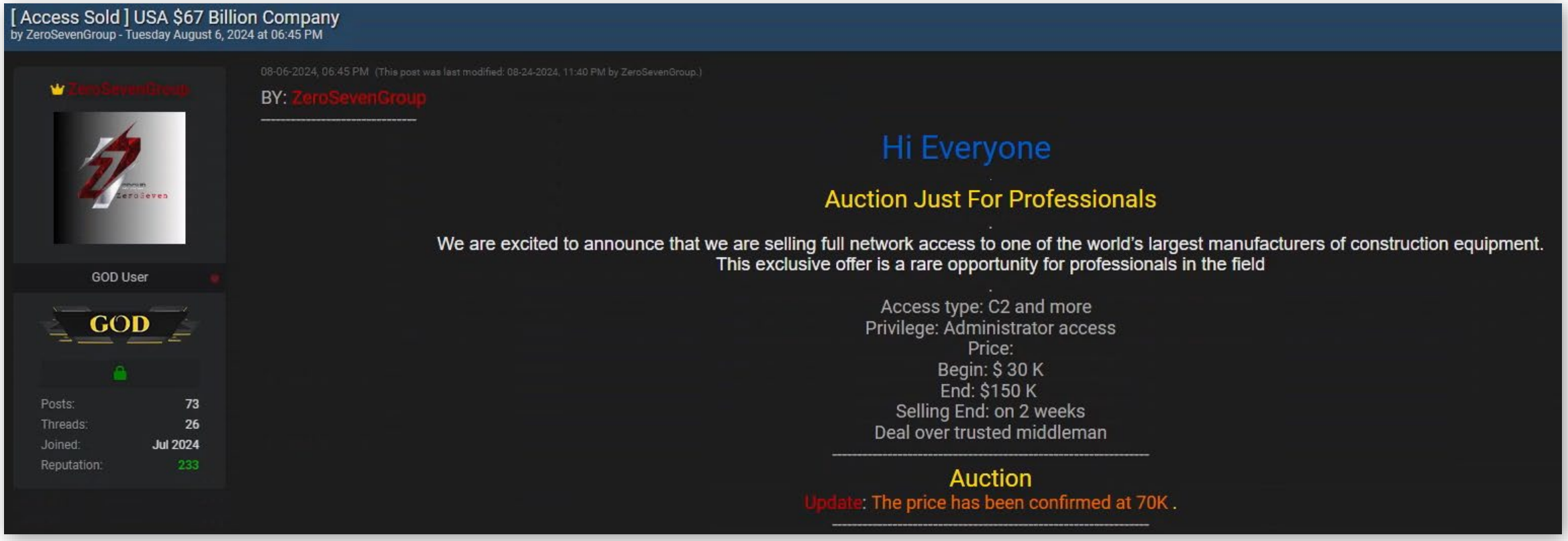
- On October 16th, 2024, **RADAR, an IAB,** offered an RDP access to Swiss corporation
- On November 23rd, 2024, the **RansomHub** group published on their official DLS on their victim list the same company
- In 2024, **RansomHub** surpassed **LockBit3.0** as the leading ransomware group, publishing 531 victims—the highest in the ransomware landscape.



RansomHub
www.[redacted].com
The [redacted] was established in 2005 and has become the premier provider of financial performance management solutions for government contractors and project focused enterprises. They are an IBM Cognos Certified Solution Provider Partner and a Deltek partner.

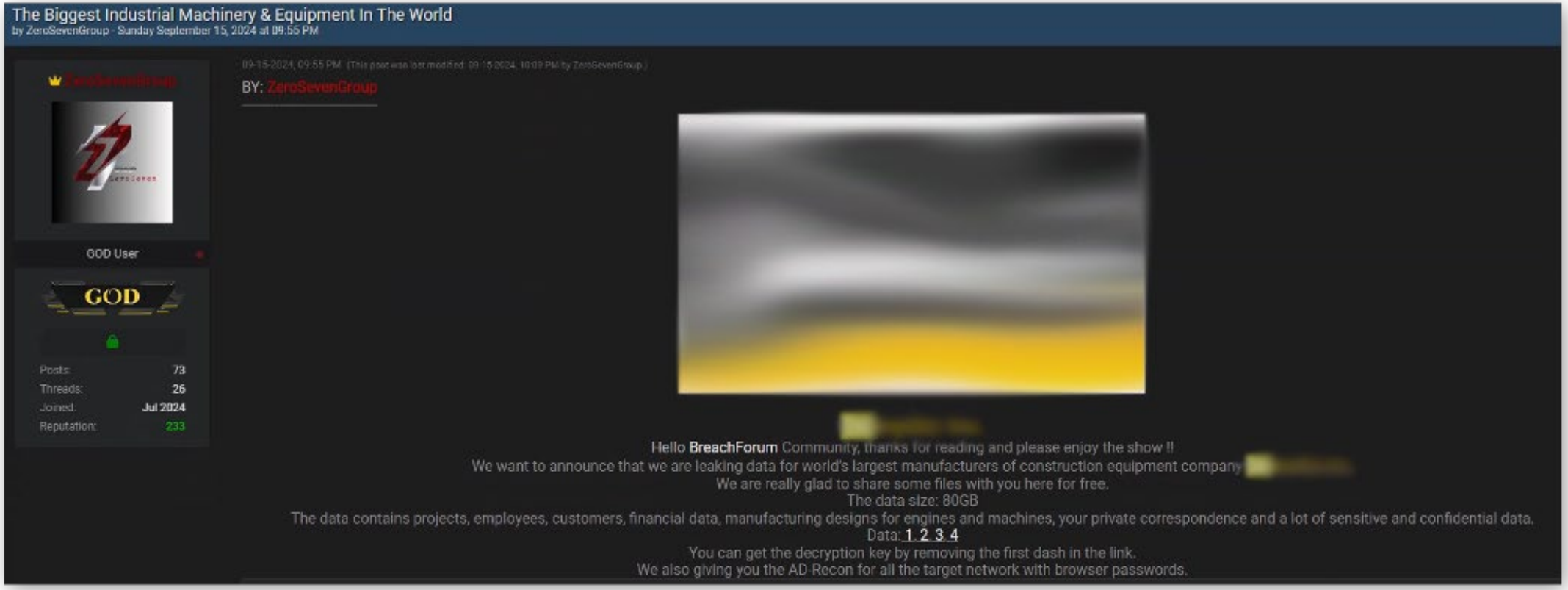
Industrial Machinery Corp - Data Leak

- **Date** – August 6, 2024
- **Threat Actor** – ZeroSevenGroup
- **Source** – BreachForums.st


[Access Sold] USA $67 Billion Company
by ZeroSevenGroup - Tuesday August 6, 2024 at 06:45 PM
ZeroSevenGroup
GOD User
GOD
Posts: 73
Threads: 26
Joined: Jul 2024
Reputation: 233
08-06-2024, 06:45 PM (This post was last modified: 08-24-2024, 11:40 PM by ZeroSevenGroup.)
BY: ZeroSevenGroup
Hi Everyone
Auction Just For Professionals
We are excited to announce that we are selling full network access to one of the world's largest manufacturers of construction equipment.
This exclusive offer is a rare opportunity for professionals in the field
Access type: C2 and more
Privilege: Administrator access
Price:
Begin: $ 30 K
End: $150 K
Selling End: on 2 weeks
Deal over trusted middleman
Auction
Update: The price has been confirmed at 70K .

Industrial Machinery Corp - Data Leak

- **Date** – September 15, 2024
- **Threat Actor** – ZeroSevenGroup
- **Source** – BreachForums.st


The Biggest Industrial Machinery & Equipment In The World
by ZeroSevenGroup - Sunday September 15, 2024 at 09:55 PM
BY: ZeroSevenGroup
GOD User
GOD
Posts: 73
Threads: 26
Joined: Jul 2024
Reputation: 233
Hello BreachForum Community, thanks for reading and please enjoy the show !!
We want to announce that we are leaking data for world's largest manufacturers of construction equipment company
We are really glad to share some files with you here for free.
The data size: 80GB
The data contains projects, employees, customers, financial data, manufacturing designs for engines and machines, your private correspondence and a lot of sensitive and confidential data.
Data: 1 2 3 4
You can get the decryption key by removing the first dash in the link.
We also giving you the AD Recon for all the target network with browser passwords.

Impact

The averagetotal cost of a data breach is

(IBM)

In 2024, the United States is the country with the highest average total cost of a data breach at

The Middle East is a close second with $8.75 million.

(IBM)

The Business Services is the most targeted sector affected by Ransomware and Data Breaches.

(Cyberint)

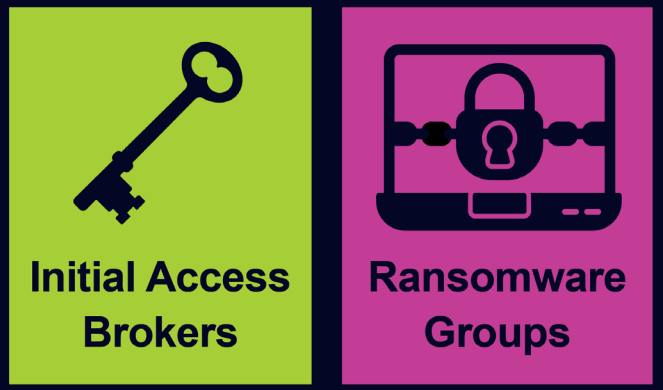
Impact

In 2024, Initial Access Brokers Activity on the Underground platform increased by

compared to 2023

(Cyberint)

Over the last years, United States is the most Targeted Country by



and all Financially motivated Threat actors

(Cyberint)

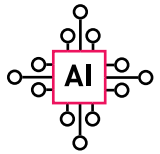
In 2024, the ransomware landscape recorded 5,414 published attacks on organizations worldwide, representing an

11%

increase compared to 2023

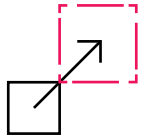
(Cyberint)

Predictions

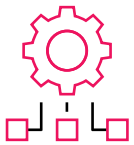


Automation & AI in Reconnaissance – Automated Phishing Attacks, Deepfake Scams, and Misinformation Campaigns

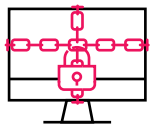
Geopolitical Motivations Behind Access Sales - Russia-Ukraine, Israel-Hamas/Hizballah/Iran, China-USA Financial Pressure



Social Engineering at Scale (ex. *Bybit* Crypto Exchange – Lazarus Heist)



Private & Public IABs Syndicates



Major Threat Actors Takedowns Will Continue – Operation Cronos, 8base, Alphv, Hive

Predictions

🔥AnonymousSudan مع KILLNET
واقفين ضد إسرائيل وضد كل من يدعم الكيان الصهيوني

🔥AnonymousSudan and KILLNET are standing against Israel and anyone who supports the Zionist Entity

🔥AnonymousSudan и KILLNET выступают против Израиля и всех, кто поддерживает Сионистскую сущность

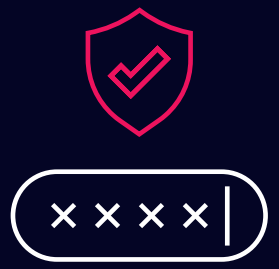
THIS WEBSITE HAS BEEN SEIZED
This domain has been seized by the Federal Bureau of Investigation in accordance with a court order pursuant to 18 U.S.C. § 1345 and 18 U.S.C. § 2521, issued by the United States District Court for the Northern District of Ohio as part of a law enforcement operation and action by:
Federal Bureau of Investigation
The United States Attorney's Office for the Northern District of Ohio
Bavarian State Criminal Police Office
Office of the Public Prosecutor General in Bamberg
National Crime Agency
NCA
National Crime Agency
For additional information, see https://www.justice.gov
Site Admins – you know who you are.
If you want to talk, contact us on Signal at +1-662-646-1561 or TOX ID
D6558476723DC998EECB84EE4A3BBAB299AADE5F22781D09FB98BD86FF40BA26D1C71F8BC69A.
Don't be the last to reach out...

THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT
This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.
We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.
Return here for more information at:
11:30 GMT on Tuesday 20th Feb.
LOCKBIT
NCA
EUROPOL
POLITIE
POLIISI

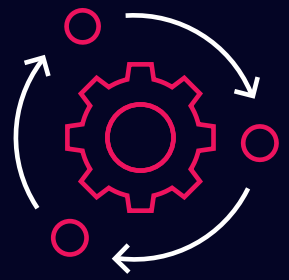
RSAC™ 2025 Conference

Now What?

Apply – Physical Security

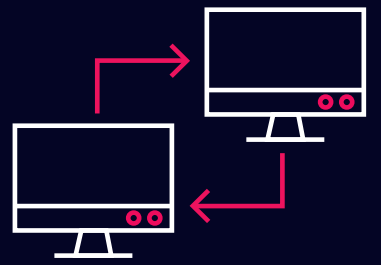


Harden Entry Points – RDP, VPN, Email



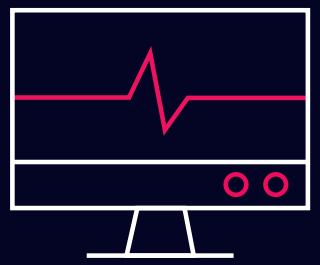
Unusual RDP/SSH logins

Limit Privilege Access



Map and Track IAB Personas

Apply – Threat Intelligence



Monitor Dark Web & Access Marketplaces

Map IABs Targets - Country, Sector, Access type, etc.

Follow Related CVEs Trends Like – RCE Vulnerabilities

RSAC™ 2025 Conference

Many Voices.
One Community.

Q & A

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You